INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

Medium Access Control Layers

For Wireless Sensor Network

Cédric Chanfreau

Promotion 58 – 2024 / 2025

29/11/2024

Plan

Table des matières

I. Wireless Sensor Network

WSNs are the most emerging technologies of 21st century. Tiny, cheap and smart sensors deployed in a physical area at denser level and networked through wireless links and internet helps these sensor nodes to act efficiently under circumstances of environmental monitoring, battlefield surveillance and regarding industry research. All this is possible just because of the advancement made by the research and scientists.

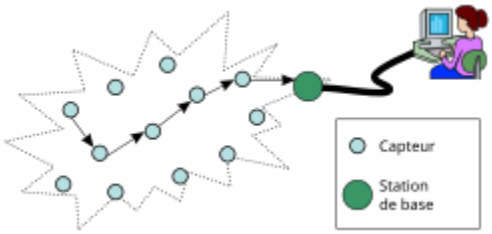

Figure 1 WSN principle

WSN typically consists of a large number of nodes which are of low power, cheap and have multifunctional sensing capabilities. These nodes are used to deploy in the field of interest at denser level. These nodes are small in size but have capabilities of processing, communication and of sensing the environmental behavior they program to sense. These distance level of nodes communications were not that much far or wide they communicate with each other at short distance through a wireless medium.

WSNs have unique characteristics which are as follows:

- **Dense Node Deployment**

Sensor nodes usually deploy densely in the field of interest to gather more data as nodes were lacking in terms of storage. Number of sensor nodes in a network can be higher depending on the environment needs they used to deploy in.

- **Battery-Powered Sensor Nodes**

Mostly the sensors deployed in the area where there it is difficult or even sometimes impossible to change or recharge the batteries of the nodes.

- **Higher Energy Consumption and Less Storage**

Sensor nodes are highly limited in terms of storage, capacity and energy.

- **Self-Configuration**

Sensor nodes are usually randomly deployed in an area where after deployment these nodes configure themselves automatically in order to make communication with each other

- **Application Specific**

Sensor networks are used to deploy in the area of specific application means that the deployment is highly depend on the application. 61

- **Unreliability**

These nodes were used to deploy under those conditions where there were many chances for the nodes to get damaged.

- **Self-Topology Configuration**

Sensor networks change their topology if any nodes get to failure, damage, and addition of new node in a network or if any of the sensor nodes get their energy drained due to some reasons.

1. MAC Layer Overview

The MAC (Medium Access Control) layer is a sublayer of Data Link Layer (Layer 2) in the OSI model. It manages access to the physical transmission medium, whether wired or wireless and ensures efficient communication across the network. With LLC (Logical Link Control) sublayer, the MAC facilitates orderly communication within a network.

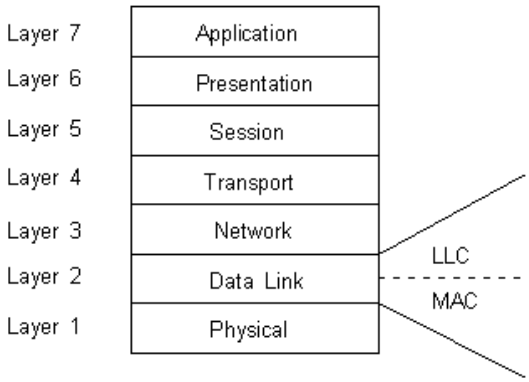

Figure 2 OSI Model

2. Role of MAC

a. Encapsulation and data transmission:
   - The MAC encapsulates higher-layer data into frames specific to the transmission medium.
   - It adds information such as synchronization preambles, Start Frame Delimiters (SFD), and Frame Check Sequences (FCS) to detect transmission errors.

b. Concurrent Access Management:
   - In shared topologies (bus, ring), the MAC regulates transmissions to prevent collisions.
   - In the event of collisions (in half-duplex mode), it handles retransmissions using defined protocols.

c. Addressing:
   - The MAC uses unique MAC addresses assigned to network interfaces to identify source and destination stations.
   - These addresses enable the delivery of data across local links through hubs, bridges, or switches.

d. Interaction with the Physical Layer:
   - It connects to the physical layer via mechanisms like the Media Independent Interface (MII).
   - The MAC acts as an abstraction layer, simplifying the complexities of physical transmission for upper layers.

3. MAC Categories

a) Contention-Based Protocols

A contention-based protocol (CBP) is a communications protocol for operating wireless telecommunication equipment that allows many users to use the same radio channel without pre-coordination. This protocol allows multiple users to share the same spectrum by defining the events that must occur when two or more transmitters attempt to simultaneously access the same channel and establishing rules by which a transmitter provides reasonable opportunities for other transmitters to operate

b) Scheduled-based MAC

Where each node follows a predetermined schedule and transmits the data according to its given time slot. The data collision is completely nullified in scheduled-based MAC.

c) Hybrid MAC

Hybrid MAC is a combination of the two protocols contention-based MAC and scheduled-based MAC to optimize the performance of wireless sensor networks. Typically, these protocols use scheduling for regular transmissions while allowing competitive access for sporadic events.

d) Cross-Layer MAC

The IEEE 802.11e standard expands on the existing IEEE 802.11 WLAN standard by incorporating Quality of Service (QoS) support. It utilizes a cross-layer approach, allowing the MAC layer to collaborate with higher layers such as the network and application layers, to provide specific services based on the application's needs.

II. MAC Protocol

In the MAC sublayer, there are several protocols such as S-MAC, B-MAC, T-MAC and PW-MAC, which are designed to manage channel access in wireless networks. These protocols aim to optimize transmissions, reduce collisions and save energy, they adapt to the specific constraints of networks, such as WSNs.

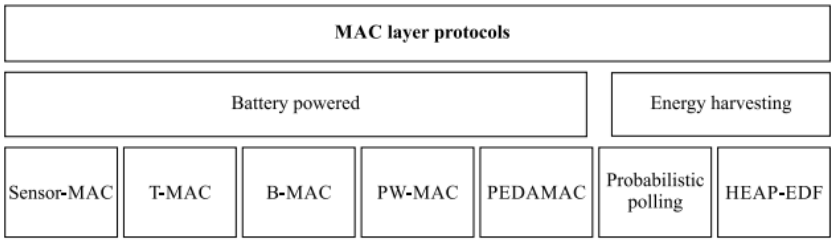

Figure 3 MAC layer protocol

1. S-MAC (Sensor MAC)

S-MAC (Sensor MAC) is a low-power, duty-cycling MAC (Media Access Control) protocol designed for wireless sensor networks. It attempts to save energy by specifically reducing the time a node spends in the active (transmitting) state and by extending the time it spends in the low-power sleep state. S-MAC achieves this by implementing a schedule-based duty-cycling mechanism. In this system, nodes coordinate their sleep and wake-up times with their neighbors and send data only at predefined time intervals. Due to this mechanism, there are fewer collisions and idle listening events, resulting in lower energy consumption.

a) Channel Access Type

During active periods, S-MAC employs CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) to manage channel access.

S-MAC uses a synchronized duty cycling mechanism to minimize energy consumption. Each node alternates between sleeping (low power) periods and active listening/transmitting periods. Neighbouring nodes coordinate their sleeping schedules using SYNC message exchanges.

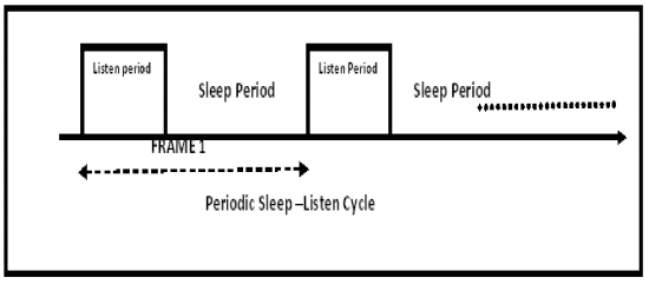

Figure 4 Periodic Sleep/Listen Period Mechanism

b) Clock Synchronization

S-MAC includes a clock synchronization mechanism. Nodes periodically exchange synchronization messages (SYNC packets) to align their sleep and listening cycles.

c) Localization capabilities

S-MAC does not directly integrate localization mechanisms. To add localization, algorithms like RSSI (Received Signal Strength Indicator) or techniques based on signal time of arrival (ToA/TDoA) must be implemented on top of S-MAC.

d) Security mechanisms

S-MAC does not natively integrate robust security mechanisms. However, extensions can be applied such as AES at the network or application layer.

e) Node mobility

S-MAC is primarily designed for static networks. In case of node mobility, losses of synchronization are frequent, leading to collisions and failed transmissions.

2. B-MAC (Berkeley MAC)

B-MAC is a low-power Medium Access Control (MAC) protocol designed specifically for wireless sensor networks. This protocol emphasizes simplicity, flexibility, and energy efficiency. Unlike more complex protocols like S-MAC, B-MAC uses a contention-based approach and a technique called Low Power Listening (LPL) to minimize power consumption and maximize sensor lifetime.

a) Channel Access Type

B-MAC uses preamble sampling. Every time a node wakes up, it checks for any activity before sending. The node also waits only for a certain amount of time to receive data. After the timeout, the node returns to sleep mode. B-MAC uses clear channel assignment and makes local policy decisions to optimize network performance. With preamble sampling, the duty cycle is reduced, which increases efficiency and throughput. Power consumption is lower due to low-power listening.

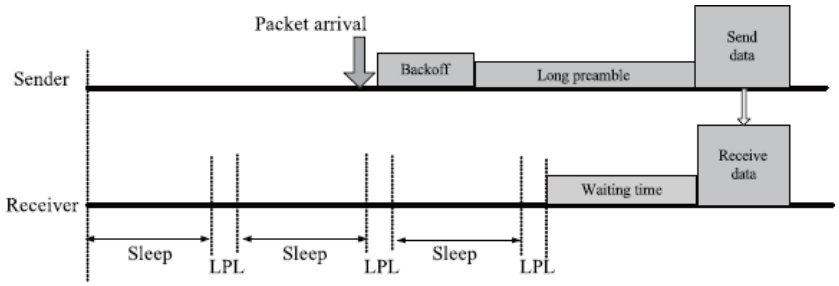

Figure 5 B-MAC Communication

b) Clock Synchronization

B-MAC does not rely on strict clock synchronization between nodes, unlike S-MAC. This makes it more flexible but can be problematic in some applications requiring synchronized transmissions.

c) Localization capabilities

Same than S-MAC

d) Security mechanisms

Same than S-MAC

3. T-MAC (Timeout MAC)

T-MAC is a part of the S-MAC protocol, designed to further reduce energy consumption in wireless sensor networks by using an adaptive approach to manage active and sleep periods. Unlike S-MAC, where the sleep and active cycles are fixed, T-MAC dynamically adapts the active durations according to the traffic requirements, making the protocol more efficient in variable traffic scenarios.

a) Channel Access Type

In T-MAC, the listen period ends when no event, such as receipt of data or sensing of activity has taken place for a threshold period. The listen period depends on current load. Transmission is based on Request-To-Send (RTS), Clear-To-Send (CTS) and acknowledgment (ACK) packets. Nodes close to the sink may have more data to send, so their listen periods are longer. The advantages are:

- RTS, CTS and ACK packets reduce collision rates and increase reliability.
- If listen periods are fixed, then nodes with less data will waste energy by idle listening.
- Energy consumption and idle listening are reduced as data can be sent in variable bursts.
- T-MAC has low sensitivity to latency, but it has a few drawbacks, such as it cannot support high data rate applications.
- Also, it has to trade-off throughput to maintain low energy consumption.

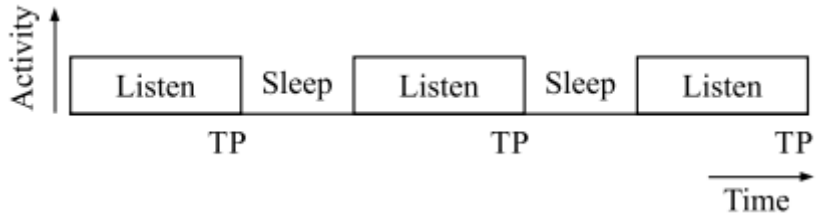

Figure 6 Adaptive listen and sleep period

b) Clock Synchronization

T-MAC retains the synchronization mechanisms inherited from S-MAC, where neighboring nodes synchronize their active cycles to avoid collisions and improve communication.

c) Localization capabilities

T-MAC, like S-MAC, does not support localization. However, it can be integrated with external algorithms to estimate node positions (RSSI or TOA).

d) Security mechanisms

T-MAC does not directly integrate security mechanisms, just like S-MAC and B-MAC. Security, including encryption and authentication, must be added in the upper layers.

4. PW-MAC (Preamble Sampling Wake-Up MAC)

PW-MAC is a protocol designed to minimize energy consumption in wireless sensor networks while reducing transmission delays, especially in low-traffic scenarios. This protocol improves on long-preamble-based protocols, such as B-MAC, by introducing an adaptive and synchronized wake-up mechanism between nodes.

a) Channel Access Type/ Clock Synchronization

In PW-MAC, the wake-up schedule of nodes can be randomized. To inform the intended transmitters, the node will send a signal upon waking up. A sender can predict the receiver's wake-up time and can wake-up simultaneously to save energy. To address timing challenges, PW-MAC has an on-demand prediction-based error correction mechanism. PW-MAC has:

- A reduced duty cycle, as it has a random node wake-up schedule.
- It has improved performance compared to S-MAC and B- MAC, as collisions can be avoided.
- Latency is less than 5% of that typical of other MAC protocols.
- Each node has to send a signal on waking-up, so the overhead of the protocol is increased, although it is low compared to other protocols.
- Also, hardware can induce errors in predicting wake-up times of the receiver.

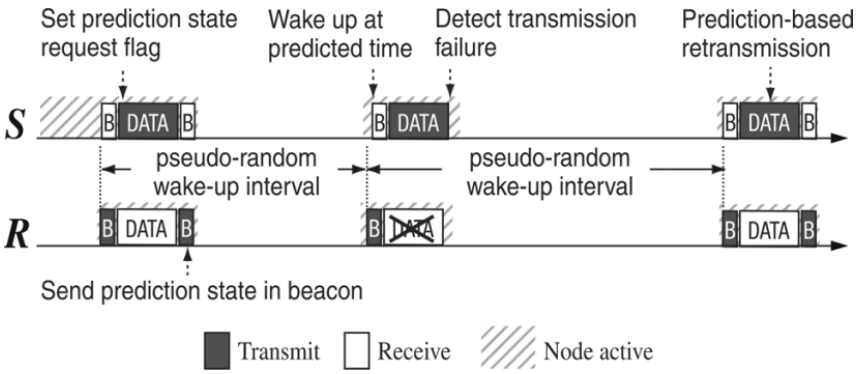

Figure 7 PW-MAC communication

5. L-MAC (Lightweight MAC)

L-MAC is a Time Division Multiple Access (TDMA)-based protocol designed to provide efficient power usage for wireless sensor networks. By dividing time into distinct time slots and assigning each node a specific slot, L-MAC aims to minimize energy consumption by avoiding collisions and retransmissions. The protocol is well-suited for networks where power efficiency and predictable communication schedules are important.

a) Channel Access Type

L-MAC operates on a TDMA scheme where the time is divided into frames, and each frame consists of a series of time slots. Each node is assigned one or more time slots in which it can transmit data.

TDMA-Based Access: Each node is assigned a dedicated time slot during which it can transmit data, ensuring that no collisions occur within a time frame.

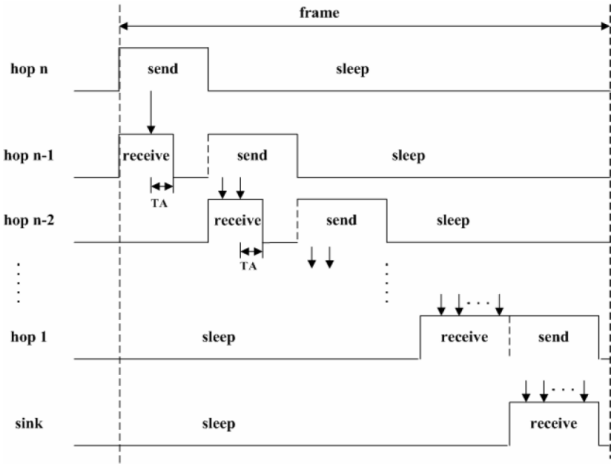

Figure 8 L-MAC Protocol

b) Clock Synchronization

In L-MAC, synchronization is achieved through the regular use of time slots. All nodes wake up at the beginning of each time slot, and time slots are coordinated across the network. This ensures that nodes are aware of when their assigned slots begin and end.

- **Implicit Synchronization**: The nodes are implicitly synchronized as they use the time slot structure to manage wake-up schedules. There is no need for complex synchronization algorithms like in some other protocols.
- **Setup Phase**: During the initial five timeframes, the network is set up. Nodes send control messages to claim time slots, and through a collision resolution mechanism, they establish their schedules.

c) Localization capabilities

L-MAC does not inherently support localization.

d) Security mechanisms

L-MAC does not have built-in security features.

6. X-MAC (Lightweight MAC)

X-MAC is an enhancement of the B-MAC protocol designed to address some of B-MAC's inefficiencies, particularly with regard to energy consumption. The key improvements in X-MAC over B-MAC revolve around the preamble structure and how nodes handle communication, reducing unnecessary energy expenditure by optimizing the way nodes wake up and listen for transmissions.

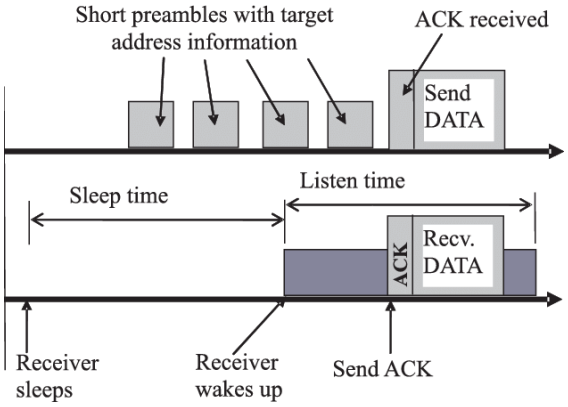

Figure 9 X-MAC Protocol

a) Channel Access Type

X-MAC, like B-MAC, operates on a contention-based mechanism using CSMA with difference in how the preamble is sent:

- **Strobed Preamble**: Instead of sending a long, continuous preamble as in B-MAC, X-MAC sends the preamble in shorter bursts with pauses between them. This improves the efficiency of the preamble transmission by preventing unnecessary transmission of preambles when the destination node is already awake and can immediately send an acknowledgment.
- **Addressing**: The preamble in X-MAC includes the address of the destination node, so that only the intended recipient wakes up to listen for the data packet.
- **Control and Data Packet**: After the acknowledgment is received from the destination node, the sender transmits the actual data packet.

b) Clock Synchronization

In X-MAC, synchronization is more efficient than in B-MAC. Since the sender only needs to send the preamble bursts rather than the full-length preamble, the synchronization overhead is reduced.

7. Z-MAC (Zebra MAC)

Z-MAC is a hybrid medium access control protocol which has its best advantages. The medium access control concept determines the channel capacity and other concepts like flow control, congestion, collisions. Z-MAC achieves high channel utilization and prevents collision between 2-hop neighbours in clusters at low cost.

a) Channel Access Type

Z-MAC is a hybrid protocol that blends the best features of both CSMA/CA (Contention-based) and TDMA (Contention-free). This hybrid approach allows Z-MAC to adapt its behavior based on the network's traffic load and the current network conditions.

- **Contention-based Phase (CSMA/CA)**: When network traffic is light, Z-MAC operates in a contention-based mode similar to CSMA/CA. In this mode, nodes use random backoff mechanisms to avoid collisions, just like traditional CSMA protocols.
- **Contention-free Phase (TDMA)**: When the network load increases and the likelihood of collisions becomes higher, Z-MAC switches to a contention-free mode. In this mode, the

protocol dynamically assigns time slots to nodes, allowing them to transmit without the risk of collision. This is akin to the TDMA protocol.

b) Clock Synchronization

Z-MAC incorporates clock synchronization during the contention-free (TDMA) phase. In this phase, nodes are assigned fixed time slots, and the system needs accurate synchronization for the transmission to happen in their respective slots without collision.

8. ALOHA

ALOHA is a contention-based protocol where nodes in the network compete to access the communication channel. It was originally designed for use in satellite networks but has since been adapted for wireless and sensor networks.

a) Channel Access Type

In ALOHA, nodes transmit data packets whenever they have data to send, without checking whether the channel is free. If a collision occurs (two nodes transmit at the same time), both packets are lost, and the nodes must retransmit their packets.

- **Pure ALOHA**: In this version, a node simply sends its packet whenever it wants. If no acknowledgment is received within a specified time window, the node assumes a collision has occurred and retries after a random backoff period.
- **Slotted ALOHA**: This version introduces time slots to the protocol. Time is divided into fixed-length slots, and nodes are required to start their transmissions at the beginning of each slot. This reduces the likelihood of collision because only the start of a time slot is considered, but if two nodes choose the same slot, a collision still occurs.
- **Contention-based**: Since there is no coordination or reservation of time slots (in pure ALOHA) or a limited reservation mechanism (in slotted ALOHA), it is considered a fully contention-based protocol.

b) Nodes Mobility

ALOHA works well in low mobility scenarios, but its performance degrades as the node mobility increases. In the case of pure ALOHA, nodes are unaware of each other's presence and can easily cause collisions, especially in a mobile environment.

- **Pure ALOHA**: Nodes can transmit at any time, making it easy for mobile nodes to participate without needing strict timing. However, this lack of coordination causes many collisions in high-density and mobile networks.
- **Slotted ALOHA**: The introduction of time slots makes ALOHA more suitable for mobile nodes, as the time synchronization minimizes collisions. However, mobile nodes must adapt to these slots, and this may require additional coordination or periodic synchronization.

9. Zigbee MAC

The ZigBee MAC (Medium Access Control) layer ensures that devices within a ZigBee network can access the radio channel efficiently and guarantees reliable data transmission. It uses the CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance) mechanism for managing channel access, which helps to prevent collisions during communication. The MAC layer serves as an interface between the physical layer and the network layer, allowing for proper synchronization and communication between devices.

a. Channel Access Type

ZigBee utilizes the **CSMA-CA** protocol for channel access. Devices listen to the channel before transmission and avoid transmitting if the channel is busy. If the channel is idle, the device transmits its data. This process helps to reduce the possibility of packet collisions and ensure reliable data delivery.

a. Clock synchronization

Beacon-based and Non-Beacon Networks: ZigBee supports two types of network configurations:

- **Beacon Mode**: In this mode, a central coordinator periodically broadcasts beacon frames to synchronize the network devices.
- **Non-Beacon Mode**: Devices communicate without synchronized beacons, offering more flexible communication for applications with lower energy requirements.

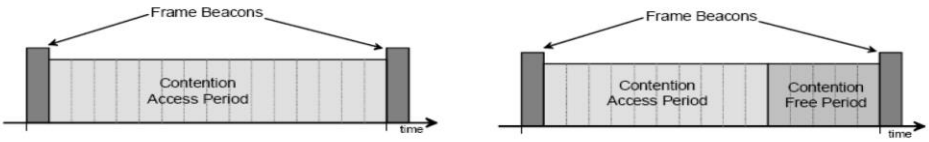

Figure 10 Tag and superframe

b. Security Mechanism

ZigBee uses AES-128 encryption to secure data during transmission, a widely accepted standard for its strength and efficiency. Mutual Authentication is employed so both sender and receiver verify each other's identity, preventing unauthorized access.

Access control ensures only authorized devices communicate within the network, while Message Integrity Codes (MICs) maintain data integrity, verifying that messages haven't been altered in transit.

ZigBee supports two security modes:

- Standard Mode: Uses shared network keys, suitable for basic applications.
- High-Security Mode: Used primarily in ZigBee PRO networks, with link keys added for specific device-to-device encryption.

c. Localization capabilities

ZigBee can provide basic localization capabilities using **Received Signal Strength Indicator (RSSI):**

- Devices estimate distances by measuring the strength of received signals.

- Although RSSI offers a simple and cost-effective solution for proximity detection, it is less precise than other localization methods like triangulation or AoA.

d. Nodes Mobility

Devices can move freely and maintain communication by connecting to the nearest router or coordinator.

III. Protocol Comparison

Protocol	Clock Synchronization	Localization Capability	Security Mechanisms	Nodes Mobility	Classification
S-MAC	Yes	No	Low	Low	Contention-based
B-MAC	No	No	Low	Low	Contention-based
T-MAC	Yes	No	Low	Low	Contention-based
PW-MAC	No	No	Low	Low	Contention-based
L-MAC	Yes (TDMA)	No	Low	Low	Schedule-based
X-MAC	No	No	Low	Low	Contention-based
Z-MAC	Yes (TDMA)	No	Low	Yes	Hybrid
ALOHA	No	No	Low	Low	Contention-based

Protocol	Energy Efficienty	Sync	Scalability
S-MAC	Moderate	Yes	Moderate
B-MAC	High	No	Moderate
T-MAC	High	Yes	Low
PW-MAC	High	No	Moderate
L-MAC	High	Yes	Moderate
X-MAC	High	No	Moderate
Z-MAC	High	Yes	High
ALOHA	Low	No	Moderate

Conclusion

In Wireless Sensor Networks, the MAC layer plays an important role in balancing energy efficiency, latency, scalability, and reliability. Each protocol is adapted to a specific use cases and constraints:

- **S-MAC** and **T-MAC** prioritize energy efficiency through sleep schedules, making them ideal for static and energy-limited networks.
- **B-MAC** and **X-MAC** focus on adaptability and simplicity, leveraging preamble sampling to reduce idle listening.
- **Z-MAC** combines the strengths of CSMA and TDMA, offering flexibility to handle varying traffic loads.
- **PW-MAC** enhances energy efficiency with advanced wake-up mechanisms, while **ALOHA** provides simplicity in low-traffic environments.
- **Zigbee MAC** stands out with its standardized, low-power design, suited for large-scale IoT applications.

These protocols demonstrate the diversity of approaches to addressing the unique challenges of WSNs. The choice of protocol depends on the application requirements, such as energy constraints, mobility, synchronization needs, and scalability. By understanding these protocols' mechanisms, we can design more efficient and tailored solutions for emerging IoT and sensor network applications.

Sources

https://fr.wikipedia.org/wiki/R%C3%A9seau_de_capteurs_sans_fil

https://en.wikipedia.org/wiki/Medium_access_control

https://en.wikipedia.org/wiki/Contention-based_protocol

https://www.geeksforgeeks.org/mac-protocol-used-in-wireless-sensor-networks/

https://ieeexplore-ieee-org.gorgone.univ-toulouse.fr/document/8259568

https://ieeexplore-ieee-org.gorgone.univ-toulouse.fr/document/5898915

https://ieeexplore-ieee-org.gorgone.univ-toulouse.fr/document/6614817

https://www.geeksforgeeks.org/s-mac-protocol-in-wsns/

https://jtit.pl/jtit/article/download/599/603/1201

https://inet.omnetpp.org/docs/users-guide/ch-sensor-macs.html

https://inet.omnetpp.org/docs/showcases/wireless/sensornetwork/doc/

https://en.wikipedia.org/wiki/Medium_access_control

https://ieeexplore-ieee-org.gorgone.univ-toulouse.fr/document/8940554

https://ieeexplore-ieee-org.gorgone.univ-toulouse.fr/document/7017481

https://en.wikipedia.org/wiki/Zebra_Media_Access_Control

https://ieeexplore-ieee-org.gorgone.univ-toulouse.fr/document/9998155

https://ieeexplore-ieee-org.gorgone.univ-toulouse.fr/document/9702081

https://ieeexplore-ieee-org.gorgone.univ-toulouse.fr/document/8371016

https://ieeexplore-ieee-org.gorgone.univ-toulouse.fr/document/5578171

https://ieeexplore-ieee-org.gorgone.univ-toulouse.fr/document/10608223